Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Collection of Law Enforcement and Crime Tool (COLECT)]

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [November 8, 2022]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Collection of Law Enforcement and Crime Tool (COLECT) enables federal, state, local, tribal, college/university, and territorial agencies to submit information to the FBI's Uniform Crime Reporting (UCR) Program for multiple data collections, including: the National Incident-Based Reporting System (NIBRS) Collection Application (NCA) and the number of Law Enforcement (LE) Employees as of October 31 Data Collection. COLECT also houses the LE Health-Related Deaths Data Collection for data quality examiners to submit officer information. In the future, COLECT may serve as the submission platform for additional UCR data collections. COLECT provides federal, state, local and tribal agencies the ability to participate in the UCR Program and reduce the time to submit and manage UCR data, eliminating costly procurements and development activities throughout the United States (US) Government. COLECT is hosted within the Amazon Web Services (AWS) Gov-Cloud environment. The underlying data collections using COLECT for data submission have separate privacy documentation, as necessary, describing the type of data in the collection and the privacy risks and mitigations associated with the specific data collections. This Privacy Impact Assessment (PIA) addresses only the privacy risks associated with the collection of user information in COLECT, not the underlying collections that use COLECT for data submission.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

COLECT allows authorized users from UCR agencies to manually submit data to the UCR Program. COLECT's authorized users include personnel from federal, state, local, college/university, tribal, and territorial government agencies with the ability to submit data to the UCR data collections and FBI personnel (employees and contractors) who support the data collections. COLECT provides users with a variety of reporting forms which correspond with the data collections available through the platform. To access COLECT, users must provide contact information for themselves and their employing agency. User information allows COLECT to determine an individual's eligibility to submit data to the UCR Program and to maintain audit logs regarding users' actions within COLECT. COLECT includes reporting forms for NIBRS, LE Employee, and LE Health-Related Deaths information. COLECT allows the submission of the data; however, NIBRS and LE Employee data will be stored in the UCR system, while LE Health-Related Deaths will be stored in its own system. Future data collections may be added to the COLECT platform. The privacy risks associated with the data collections are addressed in privacy documentation specific to the data collections and are not the

subject of this PIA.[1] COLECT is accessible via the Law Enforcement Enterprise Portal (LEEP).[2] To access COLECT, users log in to LEEP and choose the COLECT icon. Once logged in to COLECT, users can enter, save, validate, and submit information to the chosen data collections. COLECT provides a no-cost mechanism through which agencies can participate in UCR Program data collections.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

	Authority	Citation/Reference
X	Statute	28 United States Code § 534
	Executive Order	
X	Federal Regulation	28 Code of Federal Regulations 0.85(e) and (f)
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

COLECT is an intake mechanism which allows authorized users to submit information to data collections managed by the UCR Program. To facilitate the submission of data, COLECT receives and maintains the user identifications (IDs) and email addresses of its authorized users from LEEP. COLECT also requires the user's first and last name, employer/agency name and originating agency identifier (ORI), telephone number, type of agency (e.g., federal, tribal), and user role. As stated above, data collections are required to have separate privacy documentation, as necessary; consequently, this PIA focuses on the user information collected by COLECT and does not address the specific data elements within UCR data collections.

[1] For example, NIBRS and LE Employee are covered by the PIA for the National Uniform Crime Reporting Program and LE Health-Related Deaths is covered by the PIA for the Law Enforcement Officers Killed and Assaulted Program.
[2] LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. The benefits of LEEP include a single sign-on for users to access various services and systems and ensuring only authenticated users have access to those systems and services. LEEP has separate privacy documentation.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	COLECT logs the name of its users for collaboration purposes.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Work e-mail address	X	A, B, C, and D	COLECT logs the work email addresses of its users.
Work phone number	X	A, B, C, and D	COLECT logs the work phone numbers of its users.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	COLECT collects the user's employing agency name, ORI, and agency contact information.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A, B, C, and D	COLECT audit logs capture information about users accessing the system.
- **User ID**	X	A, B, C, and D	
- **User passwords/codes**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **IP address**	X	A, B, C, and D	
- **Date/time of access**	X	A, B, C, and D	
- **Queries run**	X	A, B, C, and D	
- **Content of files accessed/reviewed**	X	A, B, C, and D	COLECT audit logs also track changes users make to incident submissions.
- **Contents of files**	X	A, B, C, and D	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	COLECT also collects the user's type of agency (e.g., federal, tribal) and user role. Through COLECT, users will also receive messages regarding data submissions, such as error and reject messages, data quality messages, and other messages regarding agencies' data submission statuses.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify): Individuals apply for a COLECT account online.					

Government sources:					
Within the Component		Other DOJ Components		Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			

Government sources:
Other (specify):

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	FBI personnel supporting the UCR Program have direct access to all information (user and data collection submissions) in COLECT.
DOJ Components			X	Users with COLECT accounts will have direct log-in access to information submitted by their agency and direct access to user information for other users within their agency.
Federal entities			X	
State, local, tribal gov't entities			X	
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

Access to COLECT is limited to authorized users. Authorized users include personnel of federal, state, local, college/university, tribal, and territorial government agencies with the ability to submit data to the UCR Program. To submit data to the UCR Program, agencies must have a UCR recognized ORI. Users with a valid UCR ORI can apply for account access to COLECT via LEEP. To receive a COLECT account, users must complete the "Account Request Page," which leverages data about its users from LEEP (user ID, email address) and requests additional information (first and last name, telephone number, employer/agency name and ORI). In addition, the users will be required to provide the user's type of agency (e.g., federal, tribal) and requested user role. Once approved for access, users are assigned a user role which controls their ability to enter, view, and manage data within COLECT.

The UCR Program controls initial COLECT account access for agencies. Once the UCR Program establishes an agency point of contact in COLECT, the point of contact is assigned an Administrator role and the appropriate ORIs associated with the user's area of responsibility. Administrators serve as account managers for their agencies. As account managers, Administrators can create, approve, update, and delete roles and privileges for their users and assign roles to users (i.e., contributor or submitter). Administrators also have the functionality assigned to contributor and submitter roles and can view the transaction history for any incidents associated with their assigned ORIs. Administrators will be able to restrict their users' access to specific data collections within COLECT.

Users assigned as incident contributors by an agency can create and update incidents on behalf of their agency, but they cannot submit incidents to the UCR Program. Contributors can view the transaction history for incidents they created.

Users assigned the submitter role can create and update incidents on behalf of their agency and indicate whether an incident for their agency is complete and submit the incident to the UCR Program on behalf of their agency. Submitters can view the transaction history for incidents they submit. All agency users will be able to download a copy of their incident submissions.

FBI personnel supporting the UCR Program and COLECT have access to information within COLECT through the Administrator role. FBI personnel supporting UCR data collections can view all entries within the system; create data for training purposes and take data through the workflow process (completion, review, data quality checks, and submission); create an incident on behalf of a requesting agency; indicate whether an incident is complete and submit an incident for the next step of the review process; inform data owners if the data needs to be updated; export data to spreadsheets; assist agencies in choosing data for inclusion in reports; view the transaction history for data; and create, approve, update, and delete user accounts. Only FBI Administrators can view the COLECT audit logs.

Database administrators are responsible for maintaining the database and can view and access the data in the COLECT database. System administrators are responsible for maintaining the software, security, and computers. System administrators do not have access to incident submissions to data collections.

Access to a specific user's information is role based and restricted to the user, other users in the

user's chain of review, and FBI personnel supporting COLECT and the UCR Program, including system and database administrators. User information is maintained to provide users and reviewers with point of contact information, to facilitate generating system reports on items such as which users and agencies have submitted data and which users and agencies have data that need to be reviewed or submitted, and to allow users to subscribe to system reports and alerts. The FBI will also leverage user information to provide messages from COLECT such as data submission errors, data quality messages, and other messages regarding agencies' data submission statuses.

Account request forms will be stored in user tables within COLECT and are only accessible to FBI system administrators and users assigned the Administrator role. Agency Administrators can only access the account request forms for their assigned ORIs.

Authorized users log in to COLECT via LEEP, which authenticates the users. Once logged in to COLECT, it controls the authorization/roles and data access controls for the users. The users, based on assigned permissions, can create, view, edit, and maintain data associated with their ORIs. The users can query incident submissions to data collections via ORI, incident number, and incident date. Users can view the data history (i.e., created, modified, deleted, and reassigned) for all the data submissions associated with their ORIs. Users with submitter or administrator roles will be able to reassign data from one contributor to another within their ORI configuration. Users will be able to sign up for various forms of email notification, including daily, weekly, bi-weekly, and monthly summary report emails. If a user is designated the Administrator role, the user can opt-in to email notifications to be notified when other users within the Administrator's assigned ORIs request access to COLECT and when a user profile is updated.

Incident submissions collected by COLECT for NIBRS and data for the LE Employee collection are submitted to the UCR system for processing, retention, and publication. The data will be submitted via web services, where COLECT sends submissions to the UCR system via a machine-to-machine interaction. Web services use private/public key certifications to authenticate the transmission of data from COLECT to the UCR system. Web services allow a machine-to-machine transmission of UCR submissions to the UCR system and messages from the UCR system to COLECT.

Information for other data collections submitted through COLECT (e.g., Health-Related Deaths) are maintained in logically separated databases in COLECT.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The FBI will not release user information for COLECT users for "open data" purposes. Data collections submitted through COLECT may release data for open data purposes. The use of data collection information is addressed in separate privacy documentation specific to the data collection.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

To receive a COLECT account, users must complete the "Account Request Page," which leverages data about its users from LEEP (user ID, email address) and requests additional information (first and last name, telephone number, employer/agency name and ORI). In addition, the users will be required to provide the user's type of agency (e.g., federal, tribal) and requested user role. The Account Request Page includes a Privacy Act statement visible to the user when creating an account. The user must check a box that states the user has read and agrees to the terms for using COLECT. COLECT also provides a link to the Privacy Act statement within the platform. This PIA and the applicable System of Records Notice listed in Section 7 provide further notice to COLECT users about how their information is collected, used, shared, and processed.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Use of COLECT is voluntary. All users voluntarily apply for account access to COLECT. By requesting a COLECT account and using the system, users consent to COLECT's maintenance and use of their information.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Users can access their information in COLECT via the user profile tab. Users can update their information and are expected to keep their information up to date. Through data collection dashboards, users can search and review incident information they submitted to UCR Program data collections via COLECT.

In addition, users may request access to their records by following the guidance provided on the FBI's website at *https://www.fbi.gov/services/records-management/foipa*. A request for access to a record from this system of records must be submitted in writing and comply with 28 Code of Federal Regulations part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 200 Constitution Drive, Winchester, VA 22602-4693; facsimile: 540-868-4995/6/7; electronically: *https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records*. The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and

dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** COLECT operates under the ATO for the UCR System, which expires on November 18, 2025. In the future, COLECT will be incorporated into the Crime Data Value Stream (CDVS) security boundary which will provide information technology (IT) security controls to all systems and applications within its boundary. The FBI is working toward an ATO for CDVS. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** COLECT operates under the ATO for the UCR System. All the security controls relevant to the UCR System and COLECT using NIST Special Publication (SP) 800-37 and FBI Office of Chief Information Officer (OCIO) policies have been reviewed and are continuously monitored in RiskVision. Information System Security Officers (ISSOs) conduct continuous evaluations, and monthly status reports are presented to the Assistant Section Chief of the Information Technology Management Section.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The UCR System underwent evaluation in February 2022. All identified critical and high vulnerabilities have been removed. Other vulnerabilities have been mitigated or placed on the Plan of Action and Milestones worksheet for further evaluation for removal or mitigation. ISSOs conduct continuous evaluations, and monthly status reports are presented to the Assistant Section Chief.

X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Audit logs are kept for one year. System Security Administrators (SSAs) monitor audit logs on a daily basis. The ISSO reviews audit logs, at a minimum, every seven days. Security personnel review audit logs using automated log aggregation toolsets.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** There is no additional training specific to this system, however for user reference, user guides and answers to frequently asked questions are available within the COLECT for the NCA and the LE Employee report form.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The UCR Operations Team, ISSOs, and the SSAs continually review the security controls for COLECT per the *FBI Security Assessment and Authorization Policy Guide* and use the NIST Special Publication 800-53, for expanded definition and guidance. The ISSO is required to review security controls annually. This includes security controls focused on assessing risk to reduce the risk of unauthorized access, use, and disclosure. The risk assessment is reviewed and updated at least annually. Confidentiality is protected through acceptable security controls addressing boundary protection/external telecommunication, transmission confidentiality and integrity, and remote access/protection of confidentiality and integrity using encryption. COLECT inherits some security controls from both the FBI's Criminal Justice Information Services (CJIS) Division Shared Enterprise Network and Data Center entities.

Users access COLECT via LEEP. LEEP mitigates the risk of unauthorized access by requiring multi-factor authentication for log in. LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. To participate in LEEP and to gain access to COLECT, users must provide six identifying pieces of information: user ID, first name, last name, agency email address, agency telephone number, and employer/agency name. LEEP provides users with access to COLECT while still maintaining the constraints of the *CJIS Security Policy* and the FBI's Information Technology and Information Systems Rules of Behavior for General Users. Access to LEEP is gained through an Identity Provider (IdP). An IdP is defined as an organization/agency that creates, maintains, and vets information about each of its authorized users for LEEP access. The IdP performs user authentication each time an individual logs in to LEEP. The IdP also assigns the attributes about the individual for a given

information technology session. These attributes are presented when the user accesses LEEP via a secure web browser session at a designated URL, which then allows the user to access Service Providers, in this case COLECT. When a user selects the COLECT icon, LEEP passes the users attributes to COLECT for authentication. Once logged in to COLECT, the system determines which information within the system the users can access. Access is determined based on the user's attributes and assigned roles as outlined in Section 4.1.

The information/data is further protected by role-based controls and access control list(s) at the group and individual level. Access to user information is restricted to the user, other users in the user's agency, other users in the user's chain of review, and FBI personnel supporting the UCR Program. User access to information within COLECT is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. System access is configured to ensure only personnel with the correct credentials may access data within COLECT. If an individual does not have specific access permissions to a particular piece of data, the individual will not be able to view that data. COLECT contains audit functions that can be used to detect improper use and/or access. COLECT logs all user and administrator actions. SSAs monitor audit logs daily. The ISSO reviews audit logs, at a minimum, every seven days. Anomalous behavior or misuse of COLECT is subject to investigation and appropriate sanction, ranging from denial of access and elimination of privileges to referral to the FBI's Inspection Division, Internal Investigations Section, for investigation of FBI employee misconduct. Audit data from COLECT is supplied to the FBI's Enterprise Security Operations Center, which has a centralized view that can correlate audit information from different FBI systems.

All individuals with access to COLECT must comply with applicable security and privacy protocols address in the *CJIS Security Policy* (available at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view), the *CJIS User Agreement*, and the *LEEP Rules of Behavior*. COLECT users acknowledge that they understand sanctions may be applied for intentional misuse of the system. General users must be knowledgeable of the *General User Security Guide (GUG)* and the privileged user must be knowledgeable of the *Privileged User Security Guide (PUG)*.

COLECT utilizes the AWS Gov-Cloud environment. Access to FBI information in the cloud infrastructure is limited to FBI personnel. Access by FBI personnel to specific FBI applications and datasets is determined at the application and dataset level. Audit logs and user login identifiers are collected and maintained by both the FBI and AWS; however, AWS personnel do not have the capability to access FBI applications or datasets, or to audit user activity therein. Data in transit is encrypted using Transport Layer Security Federal Information Processing Standard 140-2 encryption, and all interconnections between the AWS Gov-Cloud and the FBI utilize firewalls and security filtering. COLECT is logically separated from other data in the cloud and resides in an FBI controlled virtual private cloud within the AWS Gov-Cloud. COLECT also relies on the CJIS Shared Enterprise Network to provide access to CJIS network, storage, logging, virus scanning, and monitoring services.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

If a user no longer requires access to COLECT their account is marked "dormant" and remains on the system for audit purposes. Dormant account data is deleted after six years or when no longer needed for investigative or security purposes, whichever is later. Audit logs are kept for one year.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

Audit log information can be retrieved by any data element in the audit log. Applications for access to COLECT can be retrieved by name, agency name, or any other data element collected with the application.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

FBI Online Collaboration Systems, **JUSTICE/FBI-004**, 82 FR 57291 (Dec. 4, 2017), available at https://www.govinfo.gov/content/pkg/FR-2017-12-04/pdf/2017-25994.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

COLECT minimizes privacy risks to its users by collecting only the minimum amount of contact information necessary to provision accounts and communicate with its users. Data elements consists of name, phone numbers, and email addresses. COLECT primarily receives user information from LEEP and the COLECT Account Request Form. Users are responsible for ensuring their contact

information is kept up to date and can update their information in their user profile, which minimizes the risk of inaccurate or stale user information. In addition, LEEP IdPs vet users annually to ensure they are still eligible for access to LEEP. When users apply for access to COLECT, FBI personnel collaborate with established agency points of contact to validate the individual applying for access works for the agency and is authorized to submit data to the UCR Program on the agency's behalf.

COLECT uses role-based access controls to protect user information by restricting access to user information. Only the user, other individuals in the user's agency, other users in the user's chain of review, and FBI personnel supporting the UCR Program can view user contact information.